

2017年3月7日

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

チェック・ポイント、『2017年サイバー・セキュリティ調査』レポートを発表

ITセキュリティ担当者の課題が明らかに

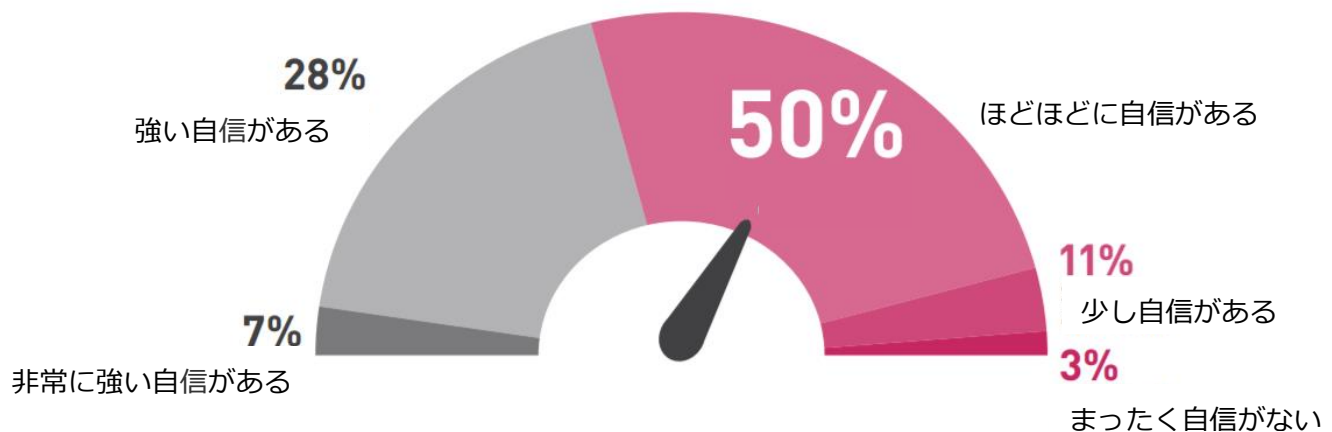
クラウドとモバイルのセキュリティに依然として高い懸念

ゲートウェイからエンドポイントまでの包括的セキュリティを提供する Check Point® Software Technologies Ltd. (NASDAQ : CHKP、インターナショナル本社：イスラエル、会長兼 CEO：ギル・シュエッド、以下チェック・ポイント) は、社員数 1,000 人以上の米国企業に勤務する IT セキュリティ担当者 1,900 人を対象にした英語版『[2017年サイバー・セキュリティ調査](#)』レポートを発表しました。

現在のビジネス環境はめまぐるしく変化し、パブリック・クラウドやプライベート・クラウドへの移行、さらなるモバイル化、個人所有のデバイスの業務利用 (BYOD) の拡大といったトレンドがある一方で、これを悪用する新たなセキュリティ脅威が出現しています。チェック・ポイントは、企業が特に懸念している課題、および IT 環境の変化が組織のセキュリティに与える影響について、IT セキュリティ担当者を対象に Crowd Research Partners 協力のもとアンケートを実施し、本レポートをまとめました。

アンケートに回答した IT セキュリティ担当者のうち、組織の全体的なセキュリティ状況について、「非常に強い自信がある」「強い自信がある」と答えたのは 35%にとどまり、65%が少なくとも「強い自信はない」と考えている実態が明らかになりました。同様の傾向は、クラウドおよびモバイルのセキュリティに関しても現れました。

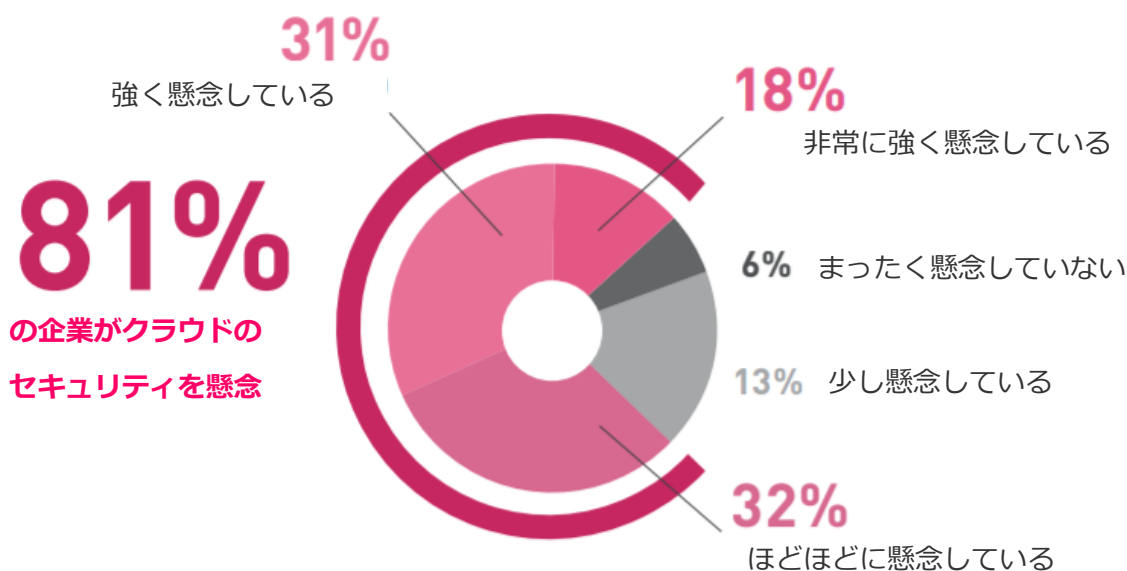
Q. 「組織の全体的なセキュリティに自信がありますか？」



高まるクラウドへの懸念

本調査では、「パブリック・クラウドの導入」が、セキュリティ上の大きな懸念事項となっていることがわかりました。パブリック・クラウドの利用について懸念を表明しているのは全体の 81%にのぼり、全体の 49% が「非常に強く懸念している」「強く懸念している」と回答しました。クラウドの導入理由としては効率性や俊敏性の向上が挙げられますが、導入を躊躇する理由は、組織の規模を問わずセキュリティが第 1 位です。IT セキュリティ担当者はクラウドでも、一般的なオンプレミスのネットワーク保護と同様に、メール・セキュリティ、Web セキュリティ、アプリケーション・セキュリティ、データ保護に加えて包括的な脅威対策を必要としています。

Q. 「パブリック・クラウドの導入において全体的なセキュリティをどのくらい懸念しますか？」



BYODの「D」はDisaster（災難）の「D」？

個人所有のデバイスの業務利用（BYDO）に関するモバイルのセキュリティについては、65%の回答者が「データ漏洩/データ損失」を主な懸念事項に挙げ、「デバイスの紛失/盗難」（61%）、「ユーザによる不正なアプリやコンテンツのダウンロード」（59%）、「業務データや業務システムへの不正アクセス」（56%）が続きました。BYDO は、メリットと同時にセキュリティ・リスクの増大をもたらす諸刃の剣です。BYDO デバイスは、セキュリティ・リスクの中身はデスクトップ PC やノート PC の場合とほぼ変わりませんが、主にコンシューマ向けに開発された製品で、業務用デバイスと比べアップデートや機種変更が頻繁なままインターネットに直接つながるため、リスクが複合的になります。モバイル・デバイスは、私用と業務用のアプリケーションが混在するケースが多く、セキュリティ対策や管理の面で、PC とは別の課題が生じます。このため、デス

クトップ PC、ノート PC、モバイル・デバイスを含むすべてのネットワーク・エンドポイントに対して、共通のセキュリティ・ポリシーを適用できる、包括的な統合ソリューションが求められています。

Q. 「BYDO に関する主なセキュリティの課題は？」



ユーザによる不正なアプリや
コンテンツのダウンロード



デバイスの紛失/盗難



業務データや業務システム
への不正アクセス

モバイル脅威への対応

モバイル脅威対策に欠かせない要素として、68%の回答者が「マルウェア対策」と回答し、「レポートिंगおよびモニタリング」(64%)、「導入の容易さ」(58%)を上回るトップでした。スマートフォンやタブレットは、同じコンピュータでも PC とはまったく別物なため、保護するためには従来のネットワーク・セキュリティ対策とは異なるアプローチが必要になります。本レポートは、モバイル・セキュリティを強化するうえでモバイル資産全体の可視化が必要と指摘しています。

Q. 「モバイル脅威対策に欠かせない要素は？」



レポートングおよび
モニタリング



58%

導入の容易さ



ネットワーク、WiFi
攻撃への防御

[『2017年サイバー・セキュリティ調査』レポート](#)は、組織全体のセキュリティを強化し、クラウド環境のデータとモバイル資産を保護するうえで、ITセキュリティ担当者が最も効果的と考えるセキュリティ対策とテクノロジーについて解説しています。また、複雑なハイブリッド・ネットワークとモバイル・デバイス全体を保護するアーキテクチャの導入方法や、セキュリティ脅威の一步先を行き、ネットワークへのサイバー攻撃を防御する方法を紹介しています。本リリースの引用元であるブログ全文は下記 URL をご覧ください。

<http://blog.checkpoint.com/2017/02/13/check-points-2017-cyber-security-survey-shows-key-concerns-opportunities-among-professionals/> (英語)

■チェック・ポイントについて ONE STEP AHEAD

チェック・ポイント・ソフトウェア・テクノロジーズ (www.checkpoint.com) は、あらゆる規模の組織に対応する世界トップクラスのセキュリティ・リーディング・カンパニーです。業界随一の検出率を誇る先進のセキュリティ対策により、お客様のネットワークをマルウェアなどの多岐にわたるサイバー攻撃から保護します。大規模ネットワークからモバイル・デバイスまでを保護する包括的なセキュリティ・アーキテクチャに加え、直感的で使いやすい総合的なセキュリティ管理ソリューションを提供しています。世界の 10 万以上の組織・企業がチェック・ポイントのセキュリティ製品を利用しています。

チェック・ポイント・ソフトウェア・テクノロジーズの全額出資日本法人、チェック・ポイント・ソフトウェア・テクノロジーズ株式会社 (<https://www.checkpoint.co.jp/>) は、1997 年 10 月 1 日設立、東京都新宿区に拠点を置いています。

©2017 Check Point Software Technologies Ltd. All rights reserved

####

《本件に関するお問い合わせ先》

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

担当 マーケティング 石黒・溝口

Tel: 03-5367-2500 / Fax: 03-5367-2501

Email: info_jp@checkpoint.com

広報代行 共同ピーアール株式会社

担当 中村・小林・上瀧

Tel: 03- 3571 – 5238 / Fax: 03- 3571-5380

Email: checkpoint-pr@kyodo-pr.co.jp